1998-01-01

Isomorphic automorphism groups of torsion-free p-adic modules

Brendan Goldsmith
Technological University Dublin, brendan.goldsmith@tudublin.ie

A. L. S. Corner

Isomorphic Automorphism Groups of Torsion-Free p-adic Modules.

A. L. S. Corner†
Worcester College
Oxford OX1 2HB
England

B. Goldsmith†
Dublin Institute of Technology
Kevin Street
Dublin, 8
and
Dublin Institute for Advanced Studies
Dublin, 4
Ireland

† This paper was supported by the joint British Council–Eolas Research Grant No. 9359.

§0. Introduction.

The question, whether two algebraic structures are isomorphic when their groups of automorphisms are isomorphic, is a fundamental but generally difficult problem in algebra. For vector spaces over fields, or more generally division rings, an affirmative answer was obtained by Rickart [5] provided that the characteristic is not equal to 2. The corresponding problem for abelian p-groups ($p \geqslant 5$) was solved affirmatively by Leptin [3] and, more recently, Liebert [4] has provided a more geometric approach which rederives Leptin's result and also handles the case of the prime $p = 3$. His proofs are lengthy and involve an intricate analysis of the situation. In the present note we solve the analogous problem for reduced torsion-free modules over the ring $\widehat{\mathbb{Z}}_p$ of p-adic integers, where $p \neq 2$. Our proof is short, and we believe it is transparent enough to serve as an introduction to the topic. The savings that we achieve are due both to simplification of some existing arguments and also, perhaps surprisingly, to the inherently simpler situation that occurs for these torsion-free modules; specifically, since all rank-1 modules are isomorphic, the key homomorphism groups which appear in our proof have a particularly simple form. Some of our simplified methods can be used to rederive Leptin's result, but they do not, unfortunately, handle the case of p-groups for $p = 3$. We have not attempted to describe all possible isomorphisms between $\operatorname{Aut} G$ and $\operatorname{Aut} \widetilde{G}$.

Our principal result is

Theorem 1. *Let G and $\widetilde{G}$ be reduced torsion-free modules over the ring of p-adic integers ($p \neq 2$) such that $\operatorname{Aut} G \cong \operatorname{Aut} \widetilde{G}$. Then $G \cong \widetilde{G}$.*

Using identical methods to those described below, it is possible to replace the $\widehat{\mathbb{Z}}_p$-modules G and $\widetilde{G}$ by homogeneous separable torsion-free abelian groups of idempotent type provided that the 2-entry in the type is ∞. In this situation the outcome is somewhat more complex and reminiscent of the situation for p-groups: the groups G and $\widetilde{G}$ will either be isomorphic or each will be isomorphic to the dual group of the other.

Our notation is standard. In particular, $ZC(\epsilon)$ denotes the centre of the centraliser of ϵ. We write mappings on the right. Relevant facts relating to torsion-free p-adic modules may be found in the monograph [2] of Kaplansky.

Finally we would like to express our thanks to the British Council and Eolas, the Irish Science and Technology agency, for the generous support without which this work would not have been possible.

§1. Extremal involutions.

In this note we shall be concerned exclusively with reduced torsion-free modules over the ring $\widehat{\mathbb{Z}}_p$ of p-adic integers, where p is a prime number $\neq 2$. The restriction on p has the effect that for any such module G the mapping $\epsilon \mapsto \frac{1}{2}(1+\epsilon)$ is a bijection from the set of all involutions in $\operatorname{Aut} G$ to the set of all idempotents in $\operatorname{End} G$. This means that to every involution $\epsilon \in \operatorname{Aut} G$ there corresponds a direct decomposition

$$G = \operatorname{Ker}(1-\epsilon) \oplus \operatorname{Ker}(1+\epsilon). \tag{1.1}$$

The involution ϵ is said to be *extremal* if one of the two summands $\operatorname{Ker}(1 \pm \epsilon)$ is indecomposable, which here amounts to being cyclic. In this situation it has been found convenient (see Liebert [4] §1) to call the cyclic summand the *line* $L(\epsilon)$ and the complementary summand the *hyperplane* $H(\epsilon)$ of the extremal involution ϵ.

We follow Liebert in basing ourselves on Rickart's observation ([5] §3; see also Fuchs [1] page 264) that extremality can be characterized in purely group-theoretical terms within the automorphism group $\operatorname{Aut} G$.

Lemma 2. *An involution ϵ in $\operatorname{Aut} G$ is extremal if and only if, for each involution $\sigma \in \mathrm{C}(\epsilon)$, $\mathrm{ZC}(\epsilon, \sigma)$ contains at most 8 involutions.*

For completeness we sketch the very easy proof. First consider a non-extremal involution ϵ in $\operatorname{Aut} G$. Then both the kernels $\operatorname{Ker}(1 \pm \epsilon)$ are directly decomposable and we may choose direct decompositions

$$\operatorname{Ker}(1-\epsilon) = A_1 \oplus A_2, \quad \operatorname{Ker}(1+\epsilon) = A_3 \oplus A_4$$

where all four summands are non-zero. We then have a direct decomposition

$$G = A_1 \oplus A_2 \oplus A_3 \oplus A_4 \tag{1.2}$$

relative to which ϵ has the matrix representation

$$\epsilon = \begin{pmatrix} \mathbf{1} & & & \\ & \mathbf{1} & & \\ & & -\mathbf{1} & \\ & & & -\mathbf{1} \end{pmatrix} = \operatorname{diag}(\mathbf{1}, \mathbf{1}, -\mathbf{1} -\mathbf{1}).$$

Let $\sigma = \operatorname{diag}(\mathbf{1}, -\mathbf{1}, \mathbf{1}, -\mathbf{1})$. Then σ is an involution commuting with ϵ, and the centraliser $\mathrm{C}(\epsilon, \sigma)$ in $\operatorname{Aut} G$ consists of all diagonal matrices $\operatorname{diag}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ with $\alpha_i \in \operatorname{Aut} A_i$. Hence its centre $\mathrm{ZC}(\epsilon, \sigma)$ consists of all diagonal matrices $\operatorname{diag}(a_1\mathbf{1}, a_2\mathbf{1}, a_3\mathbf{1}, a_4\mathbf{1})$ where the a_i are p-adic units; and it follows that $\mathrm{ZC}(\epsilon, \sigma)$ contains $2^4 = 16$ involutions. On the other hand, if ϵ is an extremal involution, one of $\operatorname{Ker}(1-\epsilon)$, $\operatorname{Ker}(1+\epsilon)$ is indecomposable, and it follows that whenever σ is an involution commuting with ϵ we get a decomposition (1.2) relative to which the matrices of ϵ, σ are as before but with the significant difference that at least one of the summands is zero, whence $\mathrm{ZC}(\epsilon, \sigma)$ contains at most $2^3 = 8$ involutions. $\square$

§2. The key lemma.

From now on let $\Phi = \overline{(\ )} : \operatorname{Aut} G \to \operatorname{Aut} \widetilde{G}$ be an isomorphism between the automorphisms groups of two reduced torsion-free $\widehat{\mathbb{Z}}_p$-modules $G, \widetilde{G}$. We fix an extremal involution ϵ in $\operatorname{Aut} G$ with line L and hyperplane H, so that

$$G = L \oplus H. \tag{2.1}$$

Correspondingly every automorphism of G has a matrix representation

$$\begin{pmatrix} \xi_{11} & \xi_{12} \\ \xi_{21} & \xi_{22} \end{pmatrix}$$

with $\xi_{ij} \in \operatorname{Hom}(G_i, G_j)$, where we have written $G_1 = L$, $G_2 = H$. In particular, if necessary absorbing a sign into ϵ, we have

$$\epsilon = \begin{pmatrix} -1 & 0 \\ 0 & \mathbf{1} \end{pmatrix}.$$

With respect to the fixed decomposition (2.1) let Δ and ∇ denote respectively all lower and all upper unitriangular matrices

$$\begin{pmatrix} 1 & 0 \\ \sigma & \mathbf{1} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & \tau \\ 0 & \mathbf{1} \end{pmatrix}.$$

It follows immediately from Lemma 2 that the image of the extremal involution ϵ is an extremal involution $\bar{\epsilon} \in \operatorname{Aut} \widetilde{G}$, so we have a corresponding direct decomposition

$$\widetilde{G} = \widetilde{L} \oplus \widetilde{H}$$

with line $\widetilde{L}$ and hyperplane $\widetilde{H}$; we give $\widetilde{\Delta}$ and $\widetilde{\nabla}$ the obvious meaning in $\operatorname{Aut} \widetilde{G}$.

We come now to the crux of the argument, which is essentially a simpler version of Satz 7 of Leptin [**3**].

Lemma 3. *Either*

(i) $\Delta\Phi = \widetilde{\Delta}$ *and* $\nabla\Phi = \widetilde{\nabla}$, *or*

(ii) $\Delta\Phi = \widetilde{\nabla}$ *and* $\nabla\Phi = \widetilde{\Delta}$.

Proof. We introduce the automorphism

$$\omega = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{Aut}\, G.$$

Note that

$$\omega \in \mathrm{ZC}(\epsilon), \quad \text{but} \quad \omega \text{ and } \epsilon\omega \notin \mathrm{ZAut}\, G.$$

Since $\Phi : \mathrm{Aut}\, G \to \mathrm{Aut}\, \widetilde{G}$ is an isomorphism

$$\overline{\omega} \in \mathrm{ZC}(\overline{\epsilon}), \quad \text{but} \quad \overline{\omega} \text{ and } \overline{\epsilon}\,\overline{\omega} \notin \mathrm{ZAut}\, \widetilde{G}.$$

Using the fact that the centre of the endomorphism algebra of a reduced torsion-free $\widehat{\mathbb{Z}}_p$-module consists of the scalar multiplications, we deduce from the first of these that

$$\overline{\omega} = \begin{pmatrix} s_1 & 0 \\ 0 & s_2\mathbf{1} \end{pmatrix}$$

where s_1, s_2 are units in $\widehat{\mathbb{Z}}_p$ or, more conveniently,

$$\overline{\omega} = s_2\overline{\rho}, \text{ where } \overline{\rho} = \begin{pmatrix} s & 0 \\ 0 & 1 \end{pmatrix},$$

where s is a p-adic unit. The non-centrality of $\overline{\omega}$ and $\overline{\epsilon}\,\overline{\omega}$ now forces $s \neq \pm 1$; therefore

$$s \neq s^{-1}. \tag{2.2}$$

Now consider an arbitrary automorphism

$$\alpha = \begin{pmatrix} 1 & 0 \\ \sigma & 1 \end{pmatrix} \in \Delta.$$

By simple (and classical) computations

$$\omega^{-1}\alpha\omega = \begin{pmatrix} 1 & 0 \\ 2\sigma & 1 \end{pmatrix} = \alpha^2, \text{ and } \epsilon\alpha = \begin{pmatrix} -1 & 0 \\ \sigma & \mathbf{1} \end{pmatrix};$$

in particular, $\epsilon\alpha$ is an involution. Therefore

$$\overline{\alpha}^2 = \overline{\omega}^{-1}\overline{\alpha}\,\overline{\omega} = \overline{\rho}^{-1}\overline{\alpha}\,\overline{\rho}, \quad (\overline{\epsilon}\,\overline{\alpha})^2 = \mathbf{1}; \tag{2.3}$$

and writing

$$\overline{\alpha} = \begin{pmatrix} \xi_{11} & \xi_{12} \\ \xi_{21} & \xi_{22} \end{pmatrix},$$

we get, on equating entries in the matrix equations (2.3), the familiar equations of Leptin,

$$\begin{array}{rcrclrcrcll}
\xi_{11}^2 & + & \xi_{12}\xi_{21} & = & \xi_{11}, & \xi_{11}^2 & - & \xi_{12}\xi_{21} & = & 1, & (2.4) \\
\xi_{11}\xi_{12} & + & \xi_{12}\xi_{22} & = & s^{-1}\xi_{12}, & \xi_{11}\xi_{12} & - & \xi_{12}\xi_{22} & = & 0, & (2.5) \\
\xi_{21}\xi_{11} & + & \xi_{22}\xi_{21} & = & s\xi_{21}, & -\xi_{21}\xi_{11} & + & \xi_{22}\xi_{21} & = & 0, & (2.6) \\
\xi_{21}\xi_{12} & + & \xi_{22}^2 & = & \xi_{22}, & -\xi_{21}\xi_{12} & + & \xi_{22}^2 & = & 1. & (2.7)
\end{array}$$

Adding the equations (2.5) gives

$$(2\xi_{11} - s^{-1})\xi_{12} = 0,$$

and similarly (2.6) leads to

$$\xi_{21}(2\xi_{11} - s) = 0.$$

By (2.2) at least one of $2\xi_{11} - s^{-1}$ and $2\xi_{11} - s$ is non-zero. Therefore at least one of $\xi_{12}, \xi_{21} = 0$. The equations (2.4) and (2.7) now reveal that the endomorphisms ξ_{11}, ξ_{22} are both idempotents and involutions, in other words $\xi_{11} = 1$, $\xi_{22} = \mathbf{1}$. Thus $\overline{\alpha} \in \widetilde{\Delta}$ or $\overline{\alpha} \in \widetilde{\nabla}$.

Noting that Δ, ∇, $\widetilde{\Delta}$, $\widetilde{\nabla}$ are all groups, we now employ a simple group-theoretical argument to show that Φ either maps all the elements of Δ into $\widetilde{\Delta}$ or all the elements of Δ into $\widetilde{\nabla}$. To this end, we may without loss consider non-trivial elements $\rho, \sigma \in \Delta$ and suppose for a contradiction that $\overline{\rho} \in \widetilde{\Delta}$, $\overline{\sigma} \in \widetilde{\nabla}$. Since the product $\rho\sigma$ lies in Δ, its image $\overline{\rho}\overline{\sigma}$ must lie in $\widetilde{\Delta}$ or $\widetilde{\nabla}$. Without loss we may assume that $\overline{\rho}\overline{\sigma} \in \widetilde{\Delta}$. It then follows that $\overline{\sigma} = \overline{\rho}^{-1}\overline{\rho}\overline{\sigma} \in \widetilde{\Delta} \cap \widetilde{\nabla} = \{\mathbf{1}\}$; and we have our contradiction.

It now follows by symmetry that Φ maps each of Δ, ∇ bodily into one of $\widetilde{\Delta}$, $\widetilde{\nabla}$. A similar argument applies to Φ^{-1}, and the result is now an easy exercise. □

§3. The proof of the theorem.

It is clear that the mapping $\sigma \mapsto \begin{pmatrix} 1 & \sigma \\ 0 & 1 \end{pmatrix}$ is a group isomorphism $\mathrm{Hom}(L, H) \to \nabla$. Since $\mathrm{Hom}(L, H) \cong H$, we obtain a group isomorphism $H \to \nabla$. We are now in a position to derive the main result, Theorem 1. We distinguish two cases, as in Lemma 3.

Case (i). Here Φ maps ∇ isomorphically onto $\widetilde{\nabla}$. By symmetry and what we have just noted, we have a group isomorphism $H \to \widetilde{H}$. This is of course an isomorphism of $\mathbb{Z}$-modules, and by a standard continuity argument it will be an isomorphism of $\widehat{\mathbb{Z}}_p$-modules. Since the lines L, $\widetilde{L}$ are automatically isomorphic, it follows that $L \oplus H$ is isomorphic to $\widetilde{L} \oplus \widetilde{H}$, which is to say that $G \cong \widetilde{G}$ as $\widehat{\mathbb{Z}}_p$-modules.

Case (ii). In this case Φ maps ∇ isomorphically onto $\widetilde{\Delta}$, and Δ isomorphically onto $\widetilde{\nabla}$. By a similar argument we have isomorphisms of $\widehat{\mathbb{Z}}_p$-modules

$$\mathrm{Hom}(H, L) \cong \widetilde{H}, \quad \mathrm{Hom}(\widetilde{H}, \widetilde{L}) \cong H.$$

Thus each of H, $\widetilde{H}$ is isomorphic to the dual of the other. This implies, as is well known, that the two modules are free of the same finite rank. For if B is a basic submodule of H, then the completeness of L forces $\widetilde{H} = \mathrm{Hom}(H, L) = \mathrm{Hom}(B, L)$, which is a product of copies of L. Consequently, $\mathrm{Hom}(\widetilde{H}, \widetilde{L})$ will be of greater cardinality than H unless $\widetilde{H} = B$ is free of finite rank. Therefore G, $\widetilde{G}$ are isomorphic free modules of the same finite rank.

This completes the proof of Theorem 1.

References

[1] L. Fuchs, *Infinite Abelian Groups*, vol II, Academic Press, New York, 1973.

[2] I. Kaplansky, *Infinite Abelian Groups*, The University of Michigan Press, Ann Arbor, 1954.

[3] H. Leptin, "Abelsche p-Gruppen und ihre Automorphismengruppen", Math. Z. 73 (1960) 235–253.

[4] W. Liebert, "Isomorphic Automorphism Groups of Primary Abelian Groups", in *Abelian Group Theory, Proceedings of the 1985 Oberwolfach Conference*, eds. R. Göbel and E. A. Walker, Gordon and Breach, New York (1987) 9–31.

[5] C. E. Rickart, "Isomorphic Groups of Linear Transformations", Amer. J. Math. 72 (1950) 451–464.